

Active Directory Nedir Ne Değildir ?

Microsoft, Windows NT'nin ardından çıkardığı Windows 2000'le birlikte yeni bir directory sistemi olarak Active Directory sistemini geliştirdi. Active Directory®, network üzerindeki nesnelere hakkında bilgileri saklayan ve bu bilgileri kullanıcılar, network yönetimi ve güvenlik için kullanmamızı sağlayan bir servistir.

Active Directory, Windows 2000 Server için tasarlandı: Windows Server 2003-2008 ve son olarak da Server 2012 ile birlikte Active Directory'de daha da geliştirildi. Yeni araçlar ve teknolojiler eklendi.

Active Directory



Network üzerindeki Nesnelere tutar

Merkezi Yönetim

- Tek bir noktadan yönetim
- Kullanıcıların tek bir oturumla izin kaynaklarına erişebilmesi

Dizin Hizmetleri İşlevleri

- Organizasyon
- Yönetim
- Kontrol

Güvenlik

- Nesnelere kimliği ve kimler tarafından kullanıldığı kontrol edilir.

Active Directory ne sağlar?

Active Directory'nin network yönetiminde kullanılan bir yönetim sistemi olduğunu ve network üzerindeki **kaynakları (resources)** yönettiğinden söz ettik. Örneğin şirket networkü içinde; bir dosyaya erişecek (izinleri olan) kullanıcıların tanımlanması gibi. İzinlerin yanı sıra Active Directory'de önemli şey **kimlik denetimi (authentication)** işlemidir. Kimlik denetimi sistem giriş ve yapılan işlemleri kullanıcı bazında kısıtlanmasında diğer bir deyişle yalnızca yetkili kullanıcıların network'ü kullanmasını sağlar.

Active Directory'ni sağladıklarını şu şekilde sıralayalım:

- Network'ün domain olarak adlandırılan birimler (alanlar) halinde düzenlenmesini sağlar.
- Kullanıcı ve grupların listesini merkezi olarak tutar.
- Kimlik denetimi (authentication) sağlar: Kullanıcı ve grupların ancak gerekli izinlere sahip olması durumunda kaynaklara erişmesini sağlar.
- Domain içindeki nesnelere, birçok özelliklerinden aranarak bulunmasını sağlar.
- Domainin OU adı verilen alt parçalara bölünmesini sağlar. Daha küçük bu birimler, yönetimin delege edilmesini sağlar.

Belli yönetim işlemlerinin yetkilendirilmesi sağlanır.

Active Directory Özellikleri

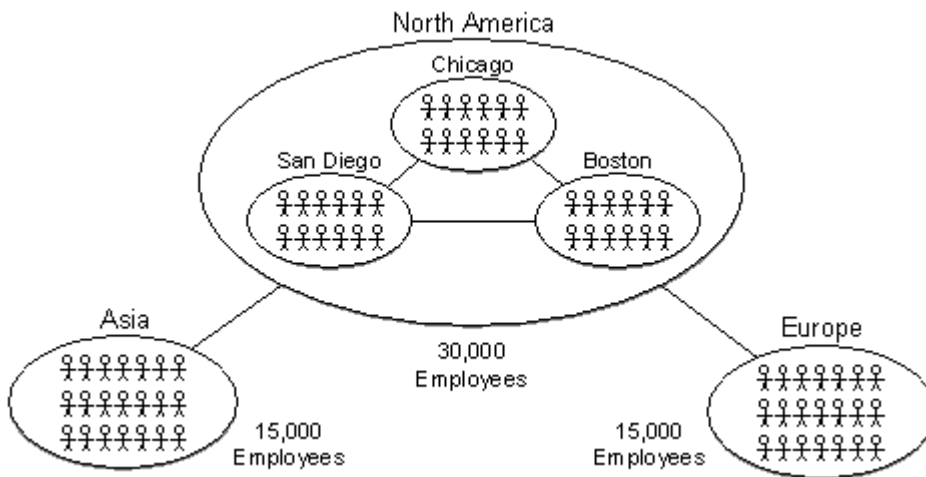
Active Directory belli özelliklere sahiptir:

Name	Size	Type
Drop		File Folder
edb001A5.log	10.240 KB	Text Docu
edb.chk	8 KB	Recovere
edb.log	10.240 KB	Text Docu
edbtmp.log	10.240 KB	Text Docu
ntds.dit	147.472 KB	DIT File
res1.log	10.240 KB	Text Docu
res2.log	10.240 KB	Text Docu
temp.edb	8.464 KB	EDB File

Merkezi Veri Depolama: Active Directory'de sistemde yer alan tüm veriler tek bir veritabanında saklanır. (NTDS.DIT). Merkezi bir veritabanı sayesinde kullanıcılar istedikleri nesneye kolayca erişebilirler.

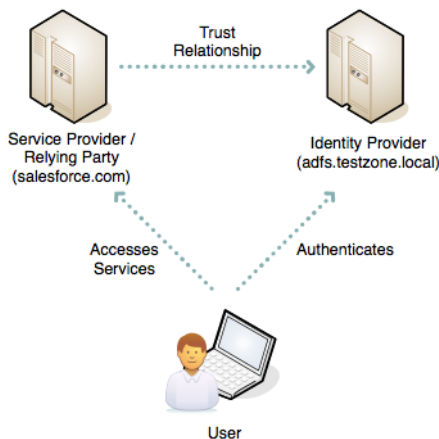
Ölçeklenebilirlik: Active Directory, farklı network gereksinimlerini karşılamak üzere ölçeklenebilme (scalability) yeteneğine sahiptir. Domain, OU ve tree yapıları sayesinde küçük, orta ve büyük ölçekli kurumsal network'lere uygulanabilir.

Genişletilebilirlik: Active Directory veritabanının yapısı genişletilebilme özelliğine sahiptir. Belli bir şemaya sahip olan veritabanına ek özellikler eklenebilir.

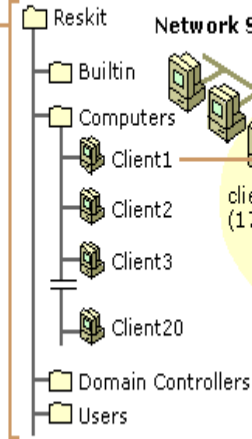
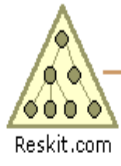


Hiyerarşik: Domain yapısı hiyerarşiktir. Bu aynı zamanda hiyerarşik bir adlandırma sistemini de destekler. DNS domain'leri gibi Internet modeliyle domain'lerin adlandırılmasını sağlar.

Bilgpro2a.senirkentmyo.com,
Bilgpro2b.senirkentmyo.com,
Bilgpro2c.senirkentmyo.com gibi.



Yönetilebilirlik: Active Directory domain'leri sistem yöneticisi tarafından birçok araçla yönetilebilir. Bu işlemler bir yerden ve bir logon ile () yapılabilir.

Active Directory Namespace

Network Subnet 172.16.72

client1.reskit.com
(172.16.72.1)**DNS Namespace**

". ." (Root)

.com

Reskit.com Zone

reskit.com

client1.reskit.com

client1.reskit.com

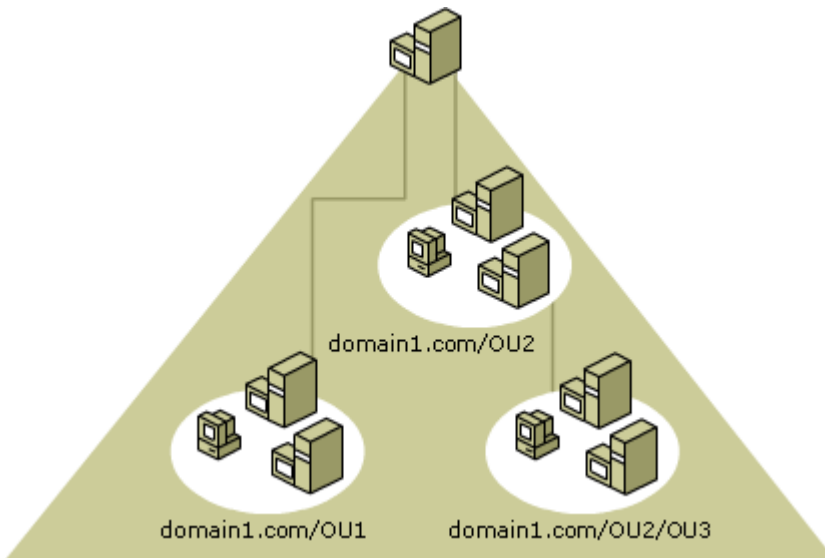
Reskit.com
Zone DatabaseDNS Host Record
for Client1.reskit.com

```

; host addresses
;
client1.reskit.com IN A 172.16.72.1
...
client20.reskit.com IN A 172.16.72.20

```

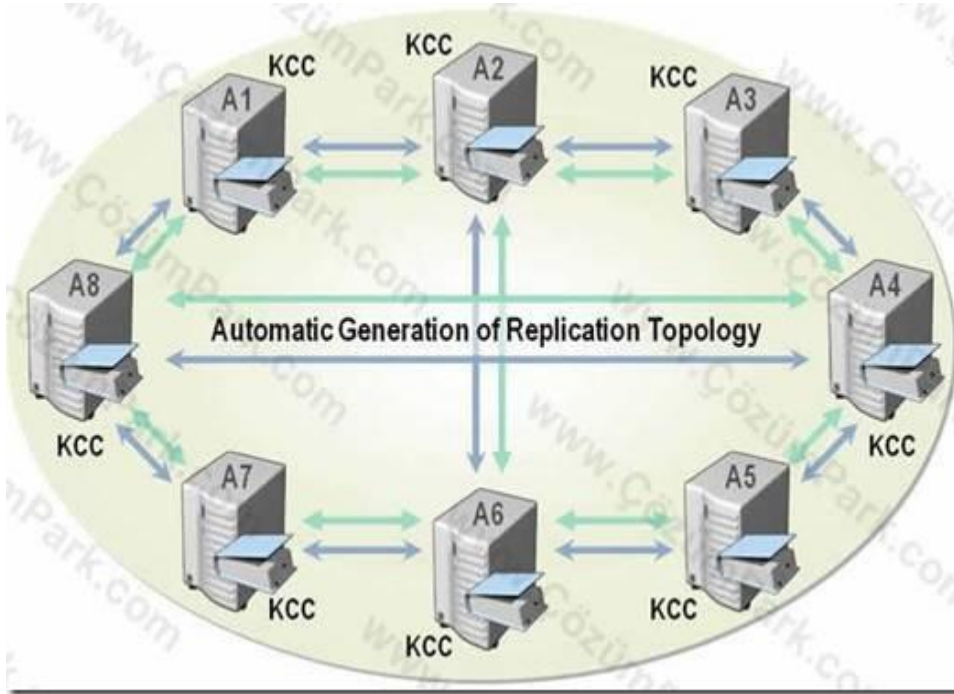
Domain Name System (DNS) ile entegrasyon: Active Directory, standart bir bir Internet (TCP/IP) servisi olan DNS ile entegre çalışır. Her ikisi de aynı hiyerarşik adlandırma yapısını kullanır. Özellikle adlandırma (adların çözülmesi) ve içerdiği server kayıtları aracılığıyla serverların bulunması işlemlerinde DNS önemli bir servistir.



Politika-tabanlı yönetim: Kullanıcı ve bilgisayarların bir site, domain ya da OU(organizational unit) içerisindeki işlemlerini kısıtlayan merkezi politikalar düzenlenebilir. Böylece kullanıcıların yalnızca izin verilen işlemleri ve bilgisayar ayarların yapması sağlanır.

Bilginin kopyalanması (replication): Active Directory bilgilerinin sürekliliğini, hataya dayanıklılığını ve yük dengelemesini sağlamak için gelişmiş bir replikasyon teknolojisine sahiptir. Bu sayede domain controller bilgisayarlar arasında domain nesnelere (veriler) kopyalanır.

Replikasyonların amacı Domain Controller'ın veritabanlarının birbirleri ile senkronize olmasını sağlamaktır. Active Directory replikasyon işlemleri karşılıklı iki domain controller arasında gerçekleşirse push ve pull replikasyon mekanizması olarak değil, pull replikasyonu şeklinde gerçekleşir. Replikasyon bir bilgisayarın diğer bir bilgisayara istekte bulunması ile başlar. Replikasyon işleminde tüm veritabanı update edilmez



sadece değişen değerler güncellenir. Domain Controller arasındaki replikasyon işleminde herhangi bir Domain Controller'da güncelleştirme olduğunda Domain Controller üzerinde "Change Notification" bilgisi oluşur. Değişikliğin olduğu Domain Controller ortamdaki diğer domain controller'lara kendisinde bir değişiklik bulunduğuna dair paket yollar. Paketi alan Domain Controller'larda bu değişikliği yapmak istediğine yönelik bir paket yollar. Karşılıklı paket alışverişinden sonra replikasyon başlar.

Active Directory sistemi belli teknolojilere dayanır:

Esnek ve güvenli kimlik doğrulama (yetkilendirme): Active Directory birçok kimlik doğrulama protokolünü kullanır. Kerberos v5, SSL v3 ve TLS v3 sertifikaları bunlardan bazılarıdır.

Güvenlik entegrasyonu: Active Directory, Windows Server sürümlerinin mevcut güvenliği ile entegre çalışır. Dizinde yer alan her bir nesne için erişim kontrol edilebilir.

Diğer izin servisleriyle birlikte çalışabilme: Active Directory LDAP v3 ve NSPI üzerine kuruludur. Bu protokolleri kullanan diğer izin servisleriyle birlikte çalışabilir.

İmzalanmış ve şifrelenmiş LDAP trafiği: Varsayım olarak tüm LDAP trafiği sayısal olarak imzalı (signed) ve şifrelidir (encrypted).

Tek bir noktadan erişim: "Single Sing On". Tek bir logon ile bütün network'e erişim. Administrator'ün bir yerden yapacağı logon işlemi ile bütün network'ü yönetmesi anlamına gelir.

Delegasyon: OU'lar sayesinde yönetim işlemlerinin bazıları (password değiştirmek, kullanıcı oluşturmak günlük işlemler) yerel birimlerdeki (OU) yetkili bir kullanıcıya devredilebilir.

Active Directory Destekli Teknolojiler

Active Directory'nin amacı standart bir sistem yönetimi (network yönetimi) sağlamaktır. Bu amaçla, Active Directory tasarımında belli standartlar söz konusudur.

Active Directory'nin desteklediği teknolojiler şunlardır:

DHCP

DHCP (Dynamic Host Configuration Protocol) servisi IP adreslerinin merkezi olarak dağıtılmasını sağlar. DHCP servisi, DNS ile (Dinamik DNS) birlikte Active Directory sistemine destek olur.

DNS

DNS (Domain Name System) servisi ise domain adlarının temelini oluşturur. Ayrıca domain controller, üye bilgisayarlar ve client bilgisayarların kayıtları DNS üzerinde tutulur.

LDAP

LDAP (Lightweight Directory Access Protocol), endüstri standardı olmuş bir directory erişim protokolüdür. Active Directory bilgilerine erişim sağlar.

Kerberos v5

Kerberos v5, domain içinde kimlik doğrulama (authentication) için kullanılan standart bir protokoldür. Kerberos v5 protokolü kullanıcıyı ve network servislerini tanımlar.

Kerberos v5 kimlik doğrulama sistemi network servislerine erişim için **ticket** bilgisini kullanır. Bu bilgiler şifrelenmiş verilerdir. Kerberos v5 servisinin önemli bir kısmını **Key Distribution Center (KDC)** oluşturur. KDC, her Domain Controller üzerinde Active Directory servisinin bir parçası olarak çalışarak parolaları ve diğer hesap bilgilerini saklar.

LDAP (Lightweight Directory Access Protocol)

Dizin; elektronik ortamda belirli türden nesnelere içerisinde bulunduran ve bu nesnelere arasında arama yapma imkanı veren yapılardır. Dizinlere örnek olarak; tutulan kişi listeleri, telefon rehberi, bir ağa dahil olan bilgisayarların listeleri ve bir şirkette çalışan personele dair tutulan kayıtlar örnek olarak gösterilebilir. Dizinlerin genel özellikleri incelendiğinde ise, yapısal depolama yaptıkları, bu depolamanın genellikle dağıtık olduğu, içerdiği nesnelere genellikle birbirlerinden bağımsız oldukları ve hiyerarşik bir düzende sıralandıkları görülecektir.

Dizin standartları 1988 yılında ISO-ITU tarafından X.500 standardı ile belirlenmiştir. X.500 standardı dizinlerin kullanımı ve erişimi ile ilgili dört farklı protokolü içerisinde barındırmaktadır. Bunlar; DAP (Directory Access Protocol-Dizin Erişim Protokolü), DSP (Directory System Protocol - Dizin Sistemi Protokolü), DISP (Directory Information Shadowing Protocol – Dizin Bilgileri Gölgeleme Protokolü) ve DOP (Directory Operational Bindings Management Protocol – Dizin İşlemsel Bağlantı Yönetim Protokolü)'dür.

LDAP (Leightweight Directory Access Protocol)ise Michigan Üniversitesinde geliştirilen, son kullanıcıların kullanımı açısından oldukça karmaşık bir yapıya sahip olan X.500 standardına uygun olarak oluşturulmuş dizinlere erişimde kullanılan DAP protokolünün hafifletilmiş biçimidir. LDAP in bir başka

oluşturulma amacı ise ilk zamanlarda DAP protokolünün sadece OSI(Open System Interconnection) referans modelini kullanmasıdır. LDAP protokolü ise TCP/IP protokolünü kullandığından dizinlere Web üzerinden de erişim imkanı sunmaktadır. Bir diğer önemli LDAP protokolü özelliği ise açık bir protokol olmasıdır. Bu sayede protokolün bilgi modeli geliştirilebilmekte ve verileri tutan sunucu çeşidinden bağımsız olarak verilere erişimin sağlanabilmektedir.

LDAP açık bir protokol olması nedeniyle, günümüzde farklı uygulamalarda sıklıkla kullanılmaktadır. Linux işletim sistemlerinde OpenLDAP programı aracılığıyla kullanılan LDAP protokolü; Windows işletim sistemlerinde ise orta ve büyük ölçekli işletmelerde yaygın kullanıma sahip olan Aktif Dizin(Active Directory) hizmeti olarak yer almaktadır. Active Directory, yaptığı birçok işlemde (yeni kullanıcı ve yeni grup tanımlama, hâlihazırdaki kullanıcı bilgilerine erişme ve bu bilgileri güncelleme, nesnelere arasında esnek sorgulama yapılabilmesi gibi işlemler) arka planda LDAP protokolünü kullanmaktadır. Ayrıca, Active Directory sunucusuna bağlanarak ihtiyaç duyulan verilerin alınması ve bu verilen düzenlenebilmesi LDAP aracılığıyla sağlanmaktadır.

LDAP veri yapıları incelendiğinde ise 3 temel özellik göze çarpmaktadır. Bunlardan birincisi LDAP verilerinin alt sınıflara ve hiyerarşik bir yapıya sahip olması, yani nesne tabanlı ve sıradüzensel bir yapıda olmasıdır. İkinci önemli özellik ise her nesnenin kendine özgü nitelik(attribute) ve değerlerden(value) meydana gelmiş olmasıdır. Bu nitelik ve değerler nesneyi dizinde bulunan diğer nesnelere farklı kılmakta ve nesneyi tanımlamaktadır. Bu nedenle nesnelere ait nitelikler birden fazla değere sahip olabilmekte ve bu değerler metin ya da ikilik sistem verileri olabilmektedir. Üçüncü önemli özellik ise depolanan her nesneyi tanımlayan tek bir belirleyici ismin(distinguished name – DN) olmasıdır.

LDAP verileri hiyerarşik düzeni, oluşturulan nesnelere içerdikleri farklı nitelikler sayesinde sağlanmaktadır. Belirli niteliklere sahip nesnelere hiyerarşik bir düzende bir araya gelerek oluşturdukları yapıya ağaç(tree) adı verilmektedir. Bir ağaçta bulunan yapılar nasıl farklı dallar aracılığıyla gövdeye ve sonrasında köke bağlanıyorsa, LDAP nesnelere de kendi içlerinde birbirlerinden farklı olsalar da ortak noktaları sebebiyle aynı grup içerisinde yer alabilmektedirler. Bu ağaç yapısının en üst kısmında kök(Root) dizin yer almaktadır. Kök dizin, organizasyonun dahil olduğu temel dizindir. Dizin hizmeti veren bir sunucunun belirleyici ismi(distinguished name) ise etki alanı ögesi(Domain Component – DC) tarafından belirlenmektedir. Etki alanı ögesi bir anlamda ağaç yapısının ana kimlik bilgilerini oluşturmaktadır ve bu ağaç yapısı içerisinde bulunan tüm nesnelere için ortaktır. Hiyerarşik yapıda etki alanı ögelerinden sonra gelen yapılar ise organizasyon üniteleridir(Organizational Unit – OU) . Organizasyon üniteleri oluşturulan nesnelere daha kolay ve daha esnek yönetimi amaçlı oluşturulmuş yapılar. Bu organizasyon üniteleri kendi içlerinde yine amaca yönelik olarak başka organizasyon üniteleri de bulundurabilmektedirler. Organizasyon üniteleri altına oluşturulan nesnelere ise kendilerine özgü ortak adlarla(Common Name – CN) birbirlerinden ayrılmaktadırlar. Yine bu ortak adlarla birbirlerinden ayrılan nesnelere kendi içlerinde farklı niteliklere sahip olabilmektedirler (soyadı, kullanıcı adı, telefon numarası, sicil numarası, IP Numarası... gibi). Aşağıdaki tabloda LDAP nesnelere ait olan bazı nitelikler ve bu niteliklerin kodları görülmektedir.

LDAP Niteliği	Nitelik Kodu	Nitelik Açıklaması	Nitelik Örneği
Organizasyon	o	Organizasyon adı	Sisteminiz İçin Çözümler
Etki alanı ögesi	dc	DNS ögesi	ceyhuncamli.com
Organizasyon ünitesi	ou	Organizasyon ünitesi adı	Ankara
Ortak ad	cn	Oluşturulan girdinin ortak adı	Kullanıcı Adı
Soyad	sn	Kullanıcı soyadı	Kullanıcı Soyadı
Kullanıcı ID	uid	Sistem giriş kimlik adı	SfS Kullanıcı Adı

LDIF (LDAP Data Interchange Format – LDAP Veri Değişim Biçimi) ise LDAP hizmeti veren sunuculara istemcilerin bağlanabilmesini ve nesnelere ait bilgileri görüntüleyebilmesini sağlayan veri değişim formatını tanımlamaktadır. Bir internet standardı olan LDIF ile dizinde tutulan nesnelere üzerinde toplu olarak işlemler yapılabilmekte, bu nesnelere ait özellikler değiştirilebilmekte ve nesne özellikleri görüntülenebilmektedir. Farklı programlama dilleri ile dizinlere erişim sağlanabilmektedir ancak bu programlama dillerinin hepsi temelde LDIF formatını kullanmaktadır. VBScript (Visual Basic Script) dili kullanılarak Aktif Dizin (Active Directory) hizmeti verilen sunucuya bağlanan ve istenilen organizasyon ünitesine dahil olan nesneye ait bilgileri görüntüleyen kod aşağıda görülmektedir.

```

1 On Error Resume Next
2
3 Set objConnection = CreateObject("ADODB.Connection")
4 Set objCommand = CreateObject("ADODB.Command")
5 objConnection.Provider = "ADsDSOObject"
6 objConnection.Open "//AD_Sunucu"
7 Set objCommand.ActiveConnection = objConnection
8 objCommand.Properties("Page Size") = 1000
9
10 objCommand.CommandText = _
11 "<LDAP://AD_Tam_yolu>;(objectCategory=User);Name;Subtree"
12 Set objRecordSet = objCommand.Execute
13 objRecordSet.MoveFirst
14
15 kullanıcı = InputBox_
16 ("Bilgilerine ulaşmak istediğiniz kullanıcının kullanıcı adını giriniz"), "Arama")
17
18 Set objUser = GetObject("LDAP://CN=" &kullanıcı &","AD_Tam_Yolu")
19
20 strGivenName = objUser.Get("givenName")
21 strSn = objUser.Get("sn")
22 strDisplayName = objUser.Get("displayName")
23 strPhysicalDeliveryOfficeName = objUser.Get("physicalDeliveryOfficeName")
24 strTelephoneNumber = objUser.Get("telephoneNumber")
25 strMail = objUser.Get("mail")
26 strWwwHomePage = objUser.Get("wwwHomePage")
27
28 MsgBox "" &kullanıcı &"' kullanıcısına ait AD veritabanı bilgileri:" _
29 &chr(13) &chr(13) _
30 &"Adı: " & strGivenName &chr(13) _
31 &"Soyadı: " & strSn &chr(13) _
32 &"Kullanıcı tam adı: " & strDisplayName &chr(13) _
33 &"Kullanıcı Ofisi: " & strPhysicalDeliveryOfficeName &chr(13)
34 &"Telefon No: " & strTelephoneNumber &chr(13) _
35 &"E-posta: " & strMail
36 &"Web Adresi: " & strWwwHomePage &chr(13) _

```

Windows Server 2012 Active Directory Kurulumu

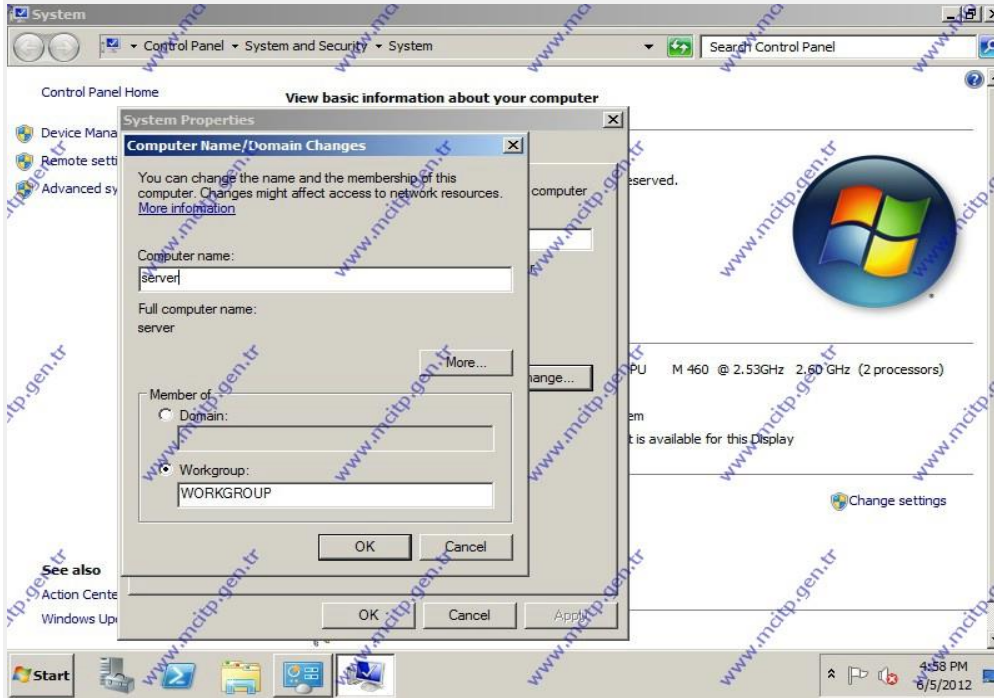
Active Directory(A.D): Merkezi yönetim yapmamızı sağlayan servisin adı. Windows 2000 Server ile gelen özelliklerin başında "Active Directory" gelir. Active Directory, ağ kaynaklarını yönetmek için geliştirilmiş bir sistemdir. Windows 2000 Server'in kuruluşunun ardından Active Directory kurularak kullanıcılar, gruplar, bilgisayarlar ve kaynakların yönetimi sağlanmaktadır.

Domain Controller(D.C): Bu servisin kurulu olduğu Servera(Yani Donanımsal olarak bir bilgisayara) verilen isimdir.

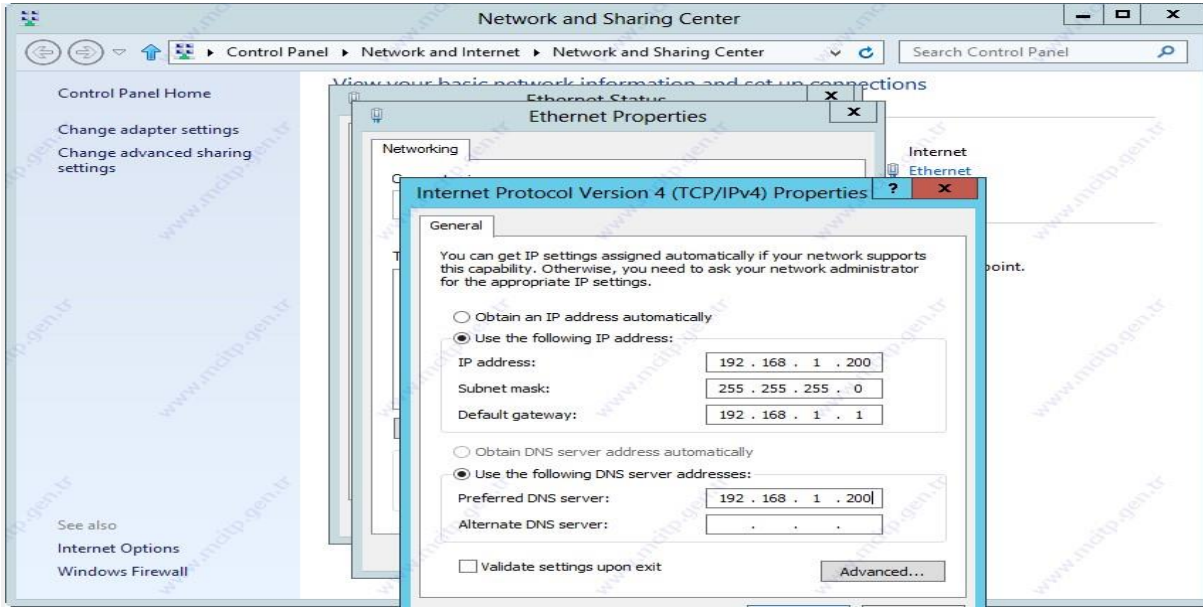
Windows 2000 serverlardan başlayan ve 2008 serverlarda da devam eden Active Directory kurma ve kaldırma sadece dcpromo ile yapılıyordu fakat server 2012 ile artık dcpromo komutu kaldırıldı. Server Manager kullanarak Active Directory kurulumunu yapabiliriz.

1.Administrator kullanıcı tanımlanmış olmalı. Administrator olmadan activedirectory kurulumu başlamaz.

2.Server adı tanımlanmalı.Server ismi kurulum yapıldıktan sonra da değiştirilebilir fakat çok tavsiye etmiyoruz bunu ,hele ortamda Additional Domain Controller (ADC) kurulacaksa server ismini değiştirmek tavsiye edilmez.



3. TCP /IP ayarlarını statik yapılandırmak.Domain Controller (DC)'lerin ip adresleri statik olmak zorunda ,eğer dinamik olarak yapılandırılırsa kurulum size ip konfigürasyonunuzu statikleştirmeniz gerektiği uyarısını verecektir.

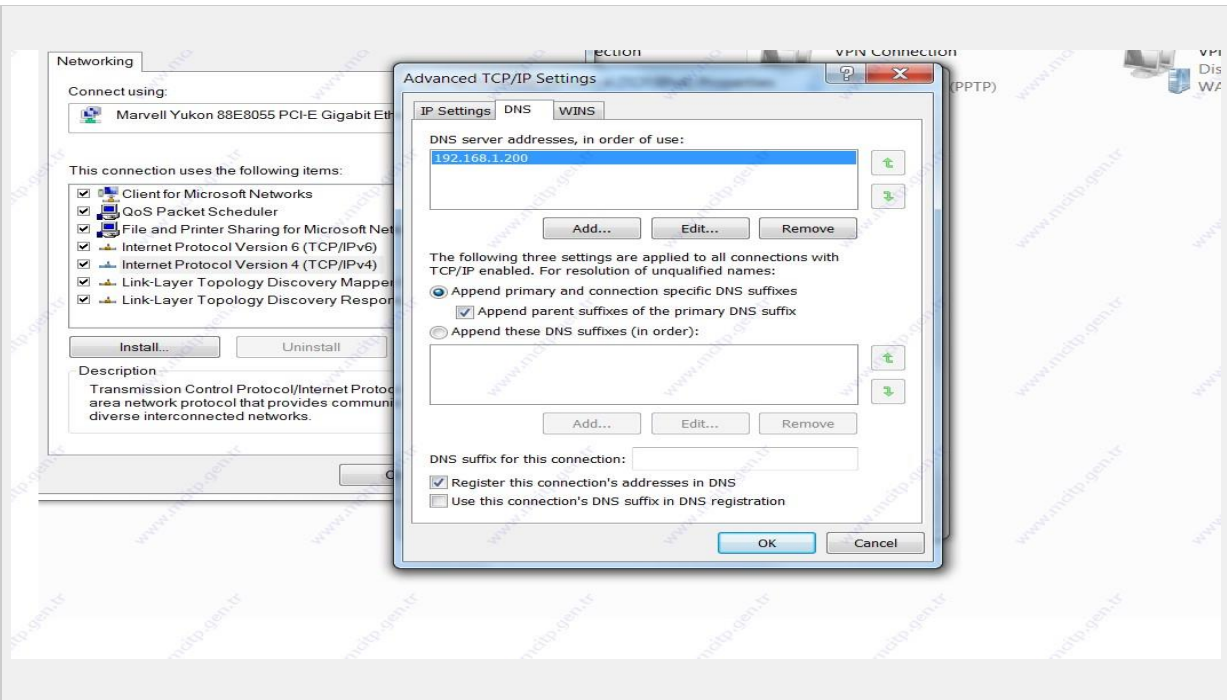


Burdaki en önemli parametre DNS ayarı diyebiliriz.

Active Directory kesinlikle DNS ile beraber çalışır.DNS çalışmazsa Active Directory 'de çalışmayacaktır.

DNS ayarı olarak Domain Controller (DC) 'nin kendisini vermek gerekmiyor ortamda çalışan başka bir DNS serverın İp adresi de verilebilir fakat hem DNS kurulumu hemde Konfigurasyonun kolaylığı açısından genelde DC ile beraber DNS de aynı server üzerine kurulur.Bu yüzden bizde DNS adresi olarak serverın kendi adresini verdik. Yani activedirectory ile beraber DNS server kurulumunu da yapacağız.

Serverinizin internet erişimi olması için varsayılan ağ geçidi(defaultgateway)olarak modemın ip adresi girilmelidir.



Ayrıca Advanced ayarlarına girip orada Registerthisconnection'saddresses in DNS ayarına checkatıyoruz.Bunu yaparak DNS üzerinde oluşması gereken Domain Controller (DC)'a ait srv (service) kayıtlarının oluşmasınısağlamış oluyoruz.

Server Managera giriyoruz ve oradan Active Directory Domain services yüklüyoruz.

Server Manager Dashboard

WELCOME TO SERVER MANAGER

1 Configure this local server

2 Add roles and features

3 Add other servers to manage

4 Create a server group

ROLES AND SERVER GROUPS

Roles: 1 | Server groups: 1 | Servers total: 1

File and Storage Services	Local Server	All Servers
1	1	1
1 Manageability	1 Manageability	1 Manageability
Events	Events	Events
Performance	Services	Services
BPA results	Performance	Performance
	BPA results	BPA results

Add Roles and Features Wizard

Before you begin

DESTINATION SERVER dc

Before You Begin

Installation Type

Server Selection

Server Roles

Features

Confirmation

Results

This wizard helps you install roles, role services, or features. You determine which roles, role services, or features to install based on the computing needs of your organization, such as sharing documents, or hosting a website.

To remove roles, role services, or features:
Start the Remove Roles and Features Wizard

Before you continue, verify that the following tasks have been completed:

- The Administrator account has a strong password
- Network settings, such as static IP addresses, are configured
- The most current security updates from Windows Update are installed

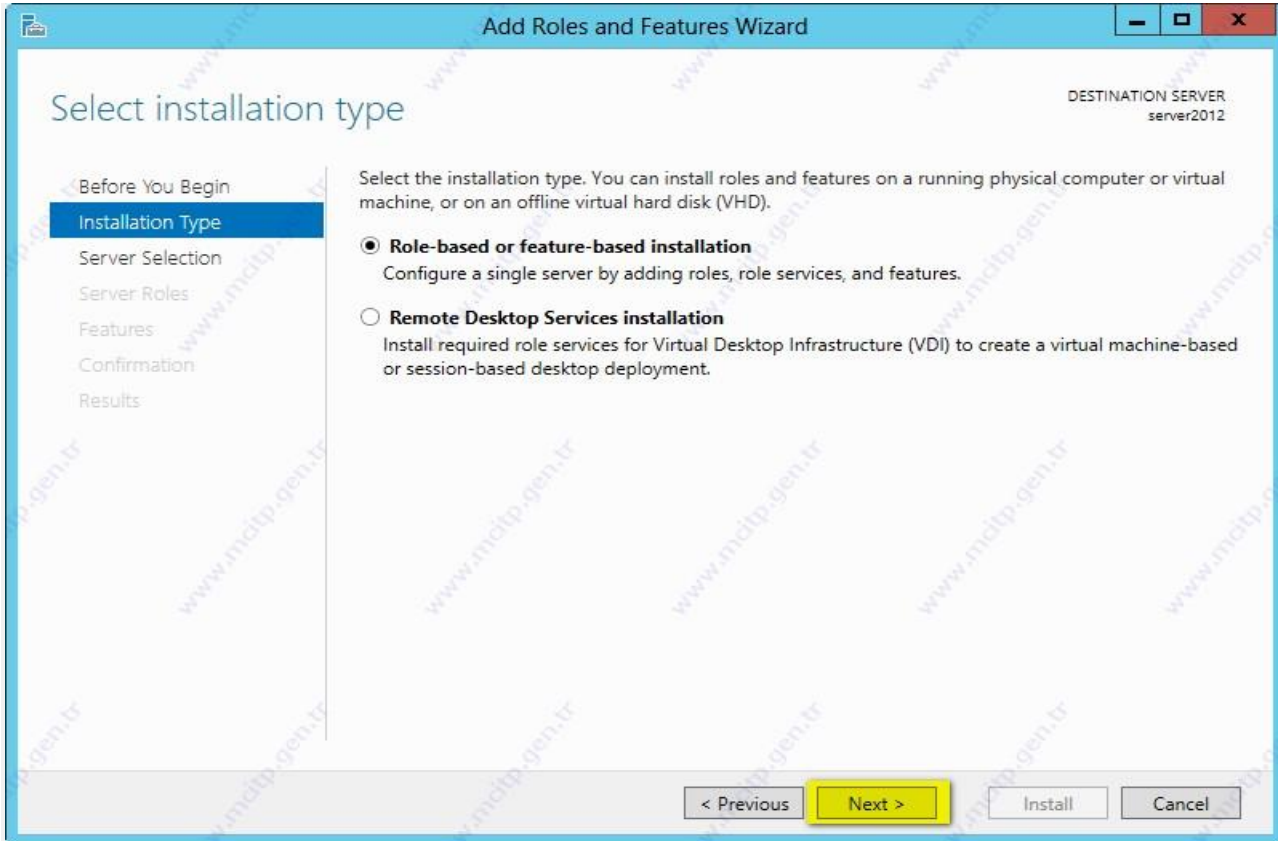
If you must verify that any of the preceding prerequisites have been completed, close the wizard, complete the steps, and then run the wizard again.

To continue, click Next.

Skip this page by default

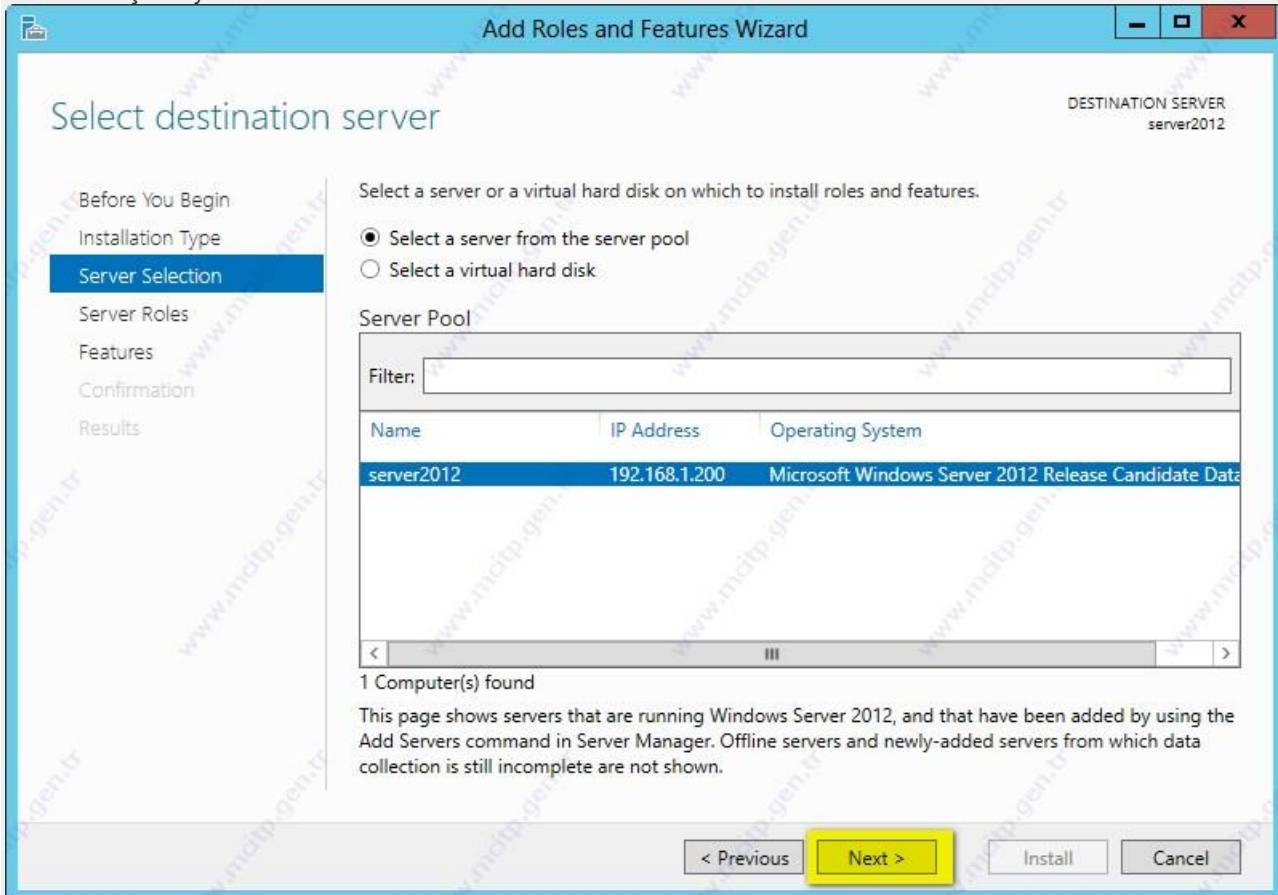
< Previous Next > Install Cancel

Gerekli bilgilendirmeleri okuduktan sonra next diyerek ilerleyelim.

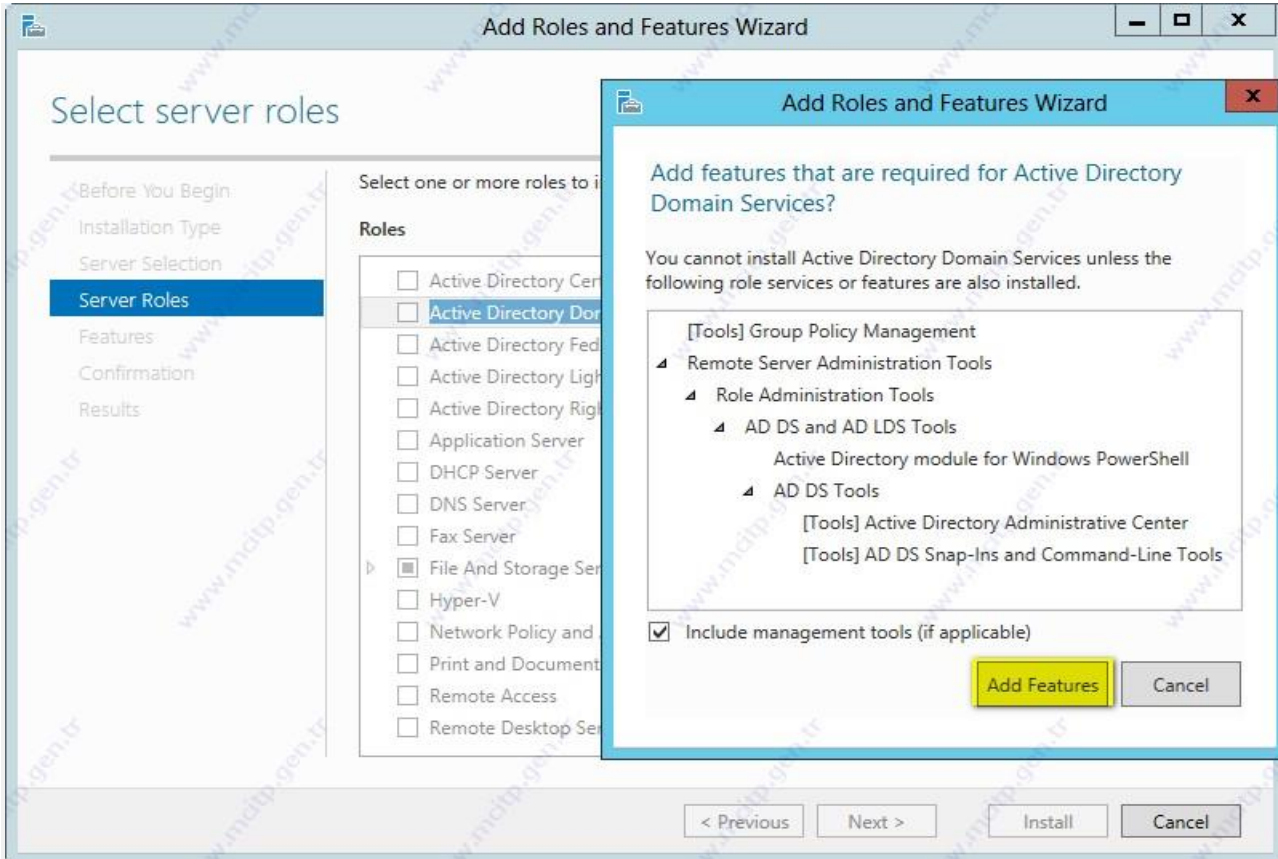


Burada

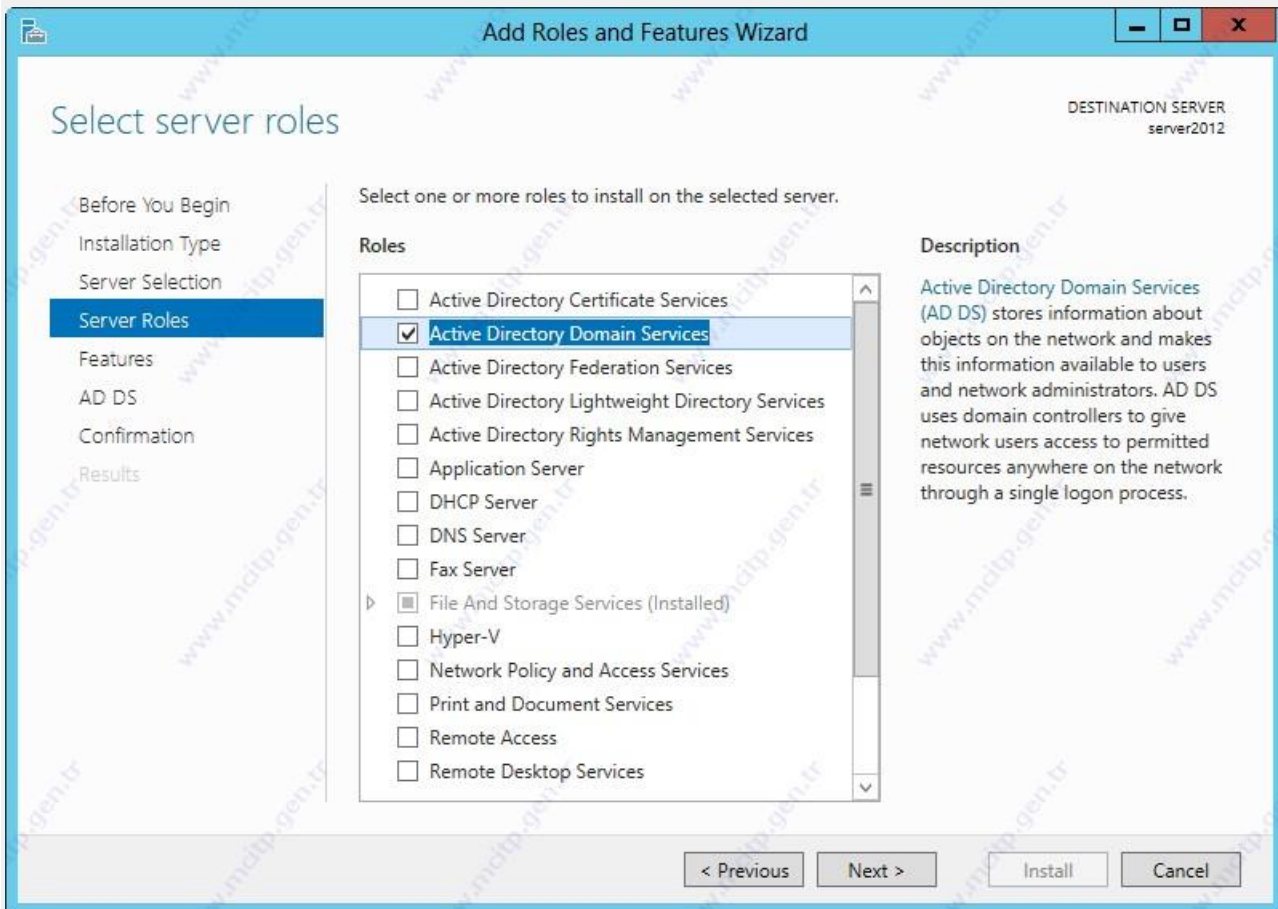
role based işaretliyoruz.



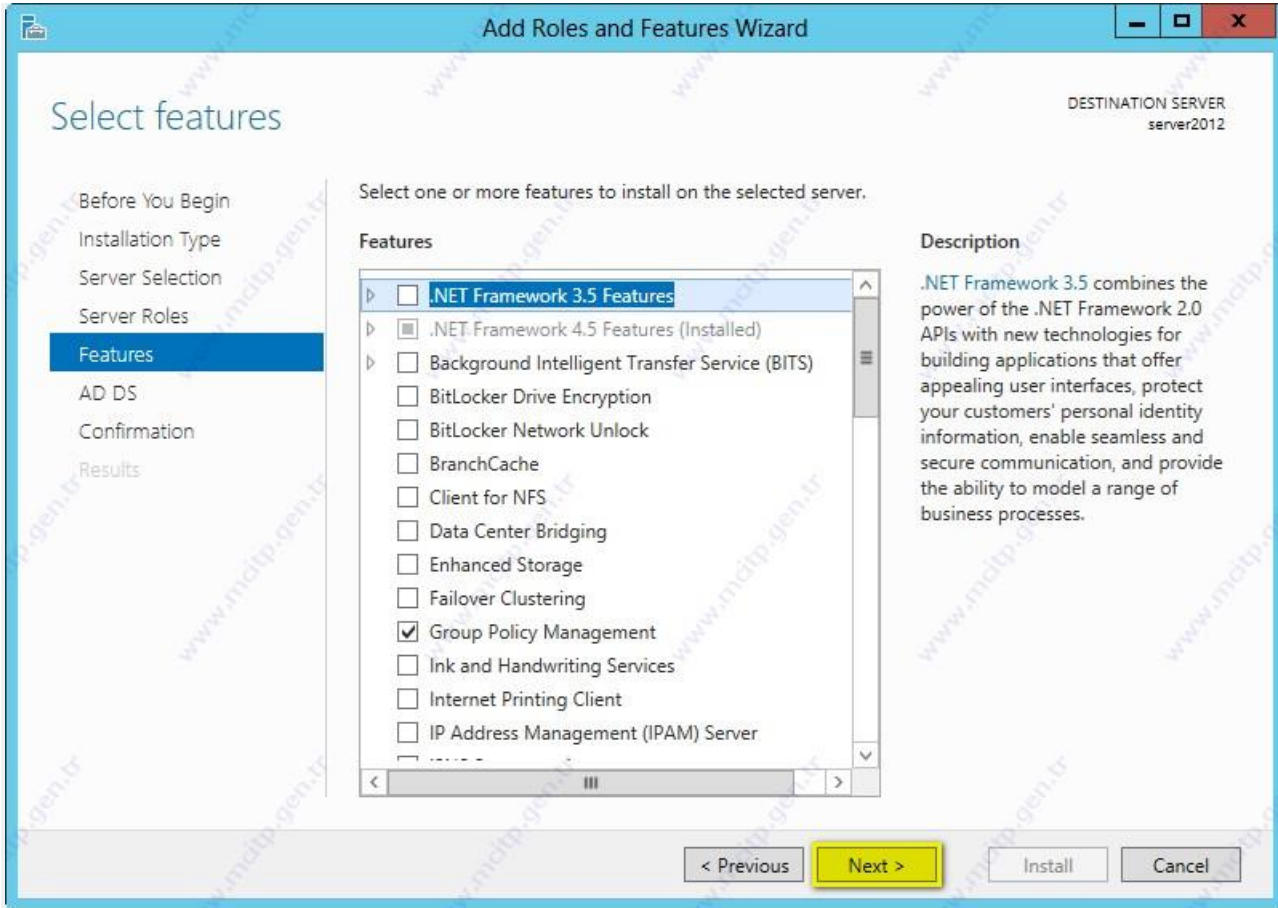
Burada hangi servera kuracağımıza karar veriyoruz. Bizvarolan server12 yiseciyoruz.



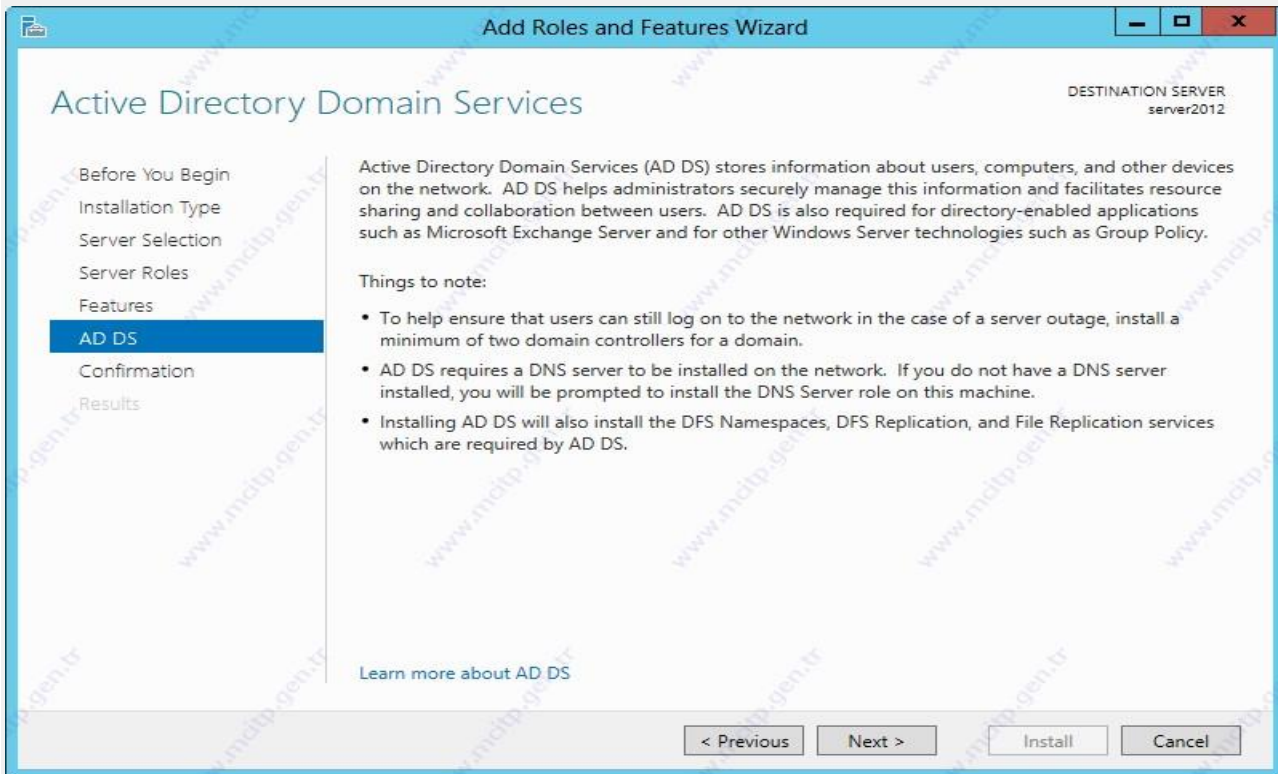
Burada Active Directory Domain Services işaretliyoruz ve o da gerekli diğer gereksinimleri ve özellikleri (features) ekliyor. Burada gerekli özelliklerin yüklenmesi için **addfeatures** diyoruz.



Next diyoruz bu aşamada .



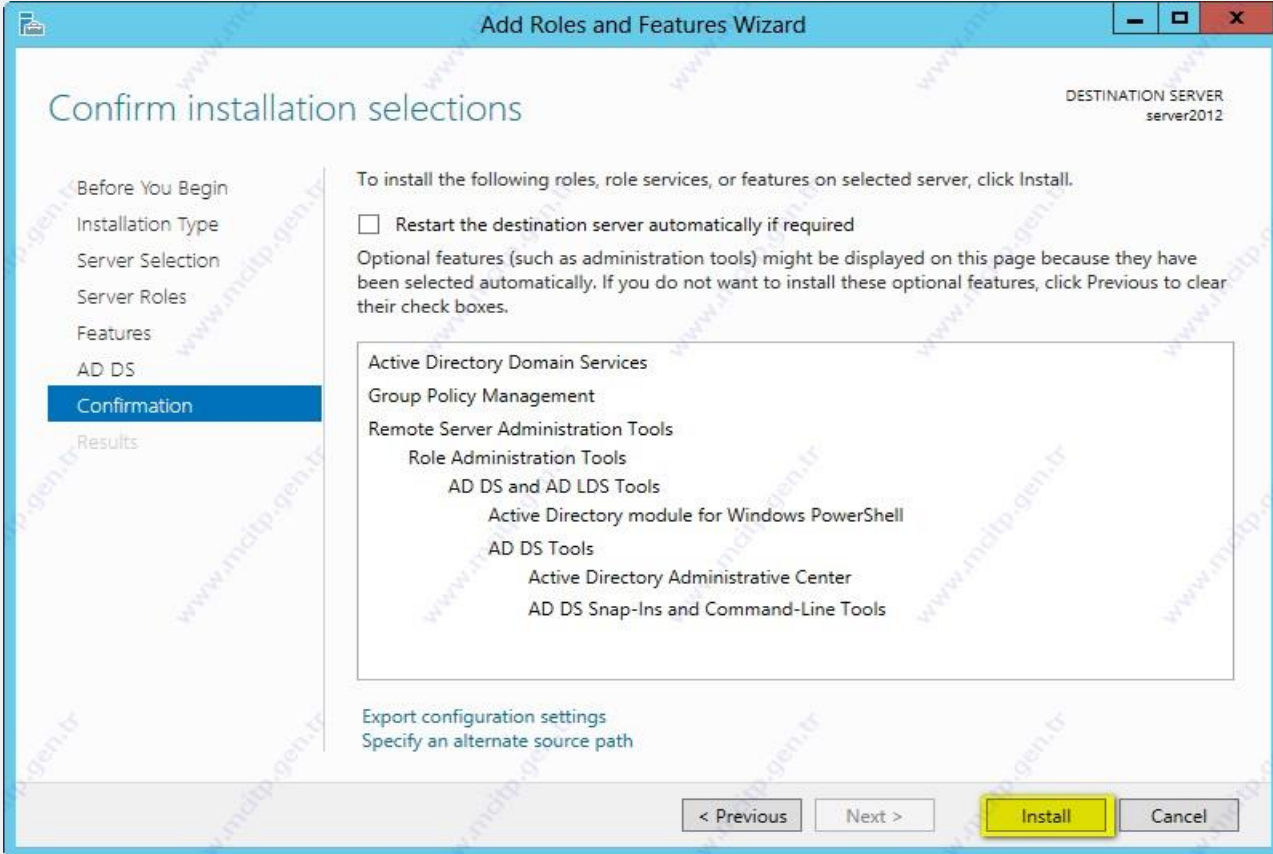
Gerekli özelliklerin (features) ların eklenip çıkarılacağı bölüm. burda da next diyoruz.



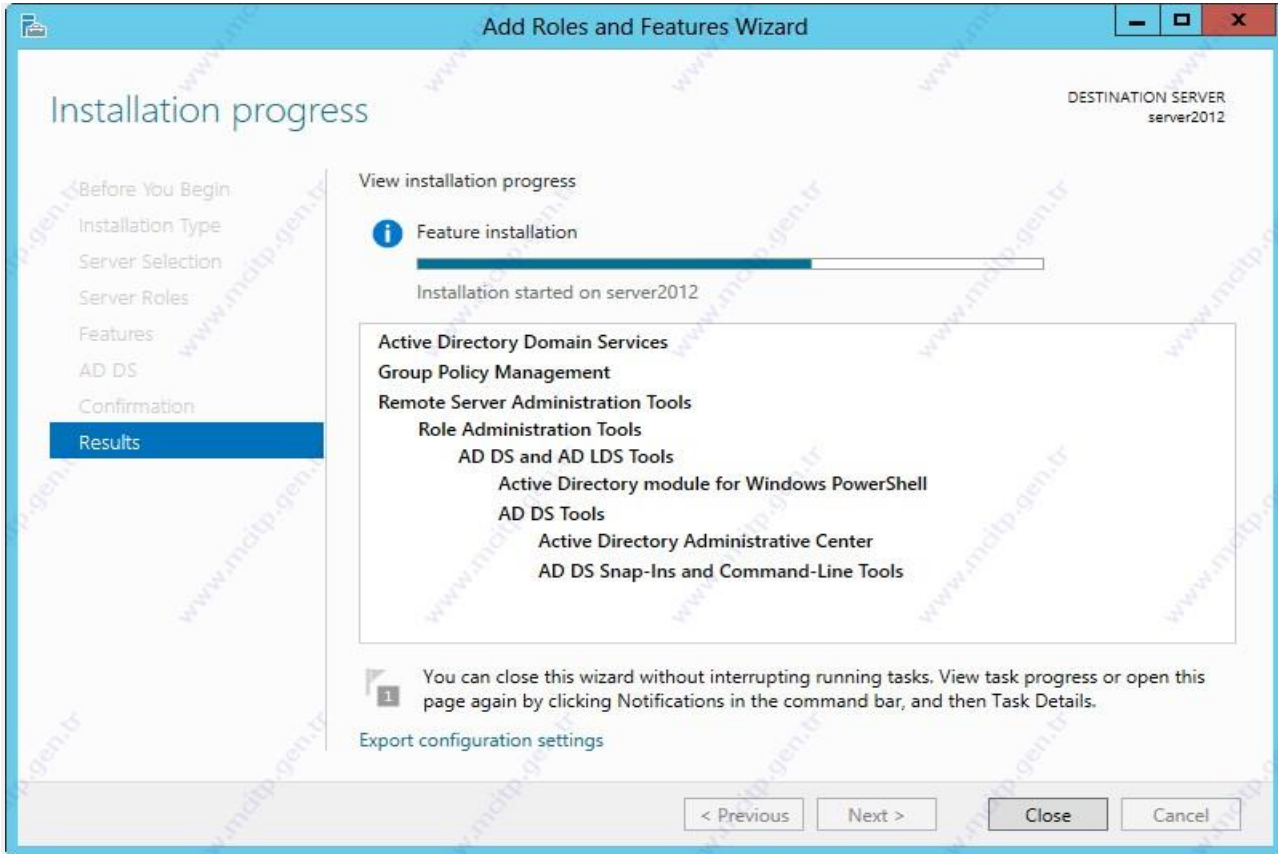
Yine Next diyoruz burada



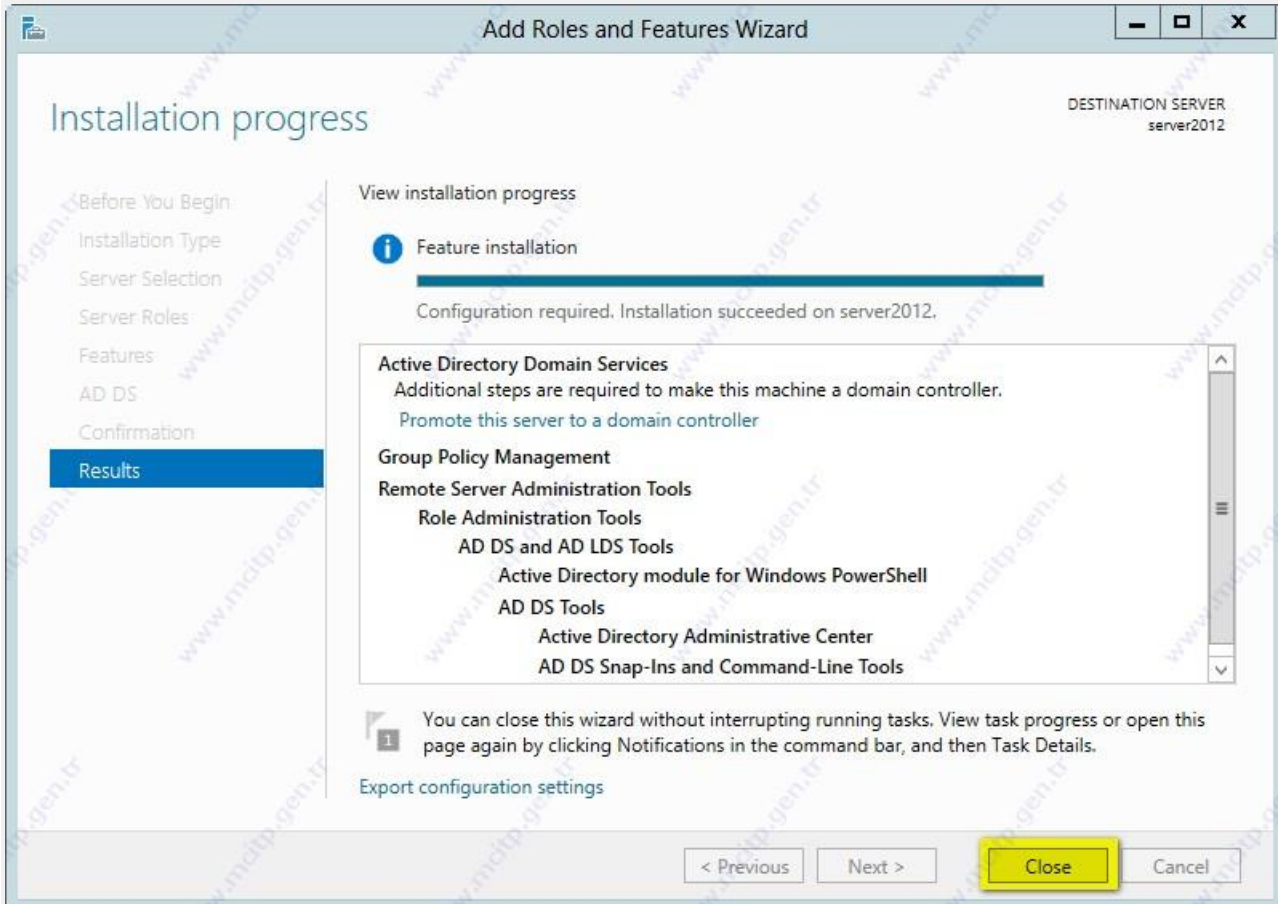
Servera Active Directory kurulduktan sonra otomatik olarak restart edecek. Yes diyerek uyarıyı kabul ediyoruz.



Kurulumun başlaması için **Install** diyoruz.



Kurulum devam ediyor.



Ve kurulum başarılı bir şekilde bitti.

Burada sadece Active Directory Domain Services eklendi.Şimdi sıra geldi Active Directory 'nin kurulmasına .Başta söylediğimiz gibi artık **DCPROMO** yok ve onun yerine **Active Directory Configuration Wizard** geldi.

Evet domain services kuruldu ardından **Server manager**'dan **AD DS** rolüne geliyoruz ve oradan **More** 'a tıkıyoruz.

SERVERS
All servers | 1 total

Configuration required for Active Directory Domain Services at SERVER2012

Server Name	IPv4 Address	Manageability	Last Update	Windows Activation
SERVER2012	192.168.1.200	Online - Cannot get BPA results	8/22/2012 11:06:06 PM	00133-30010-00805-AA582 (Activated)

EVENTS
All events | 0 total

Server Name	ID	Severity	Source	Log	Date and Time
-------------	----	----------	--------	-----	---------------

Ardından

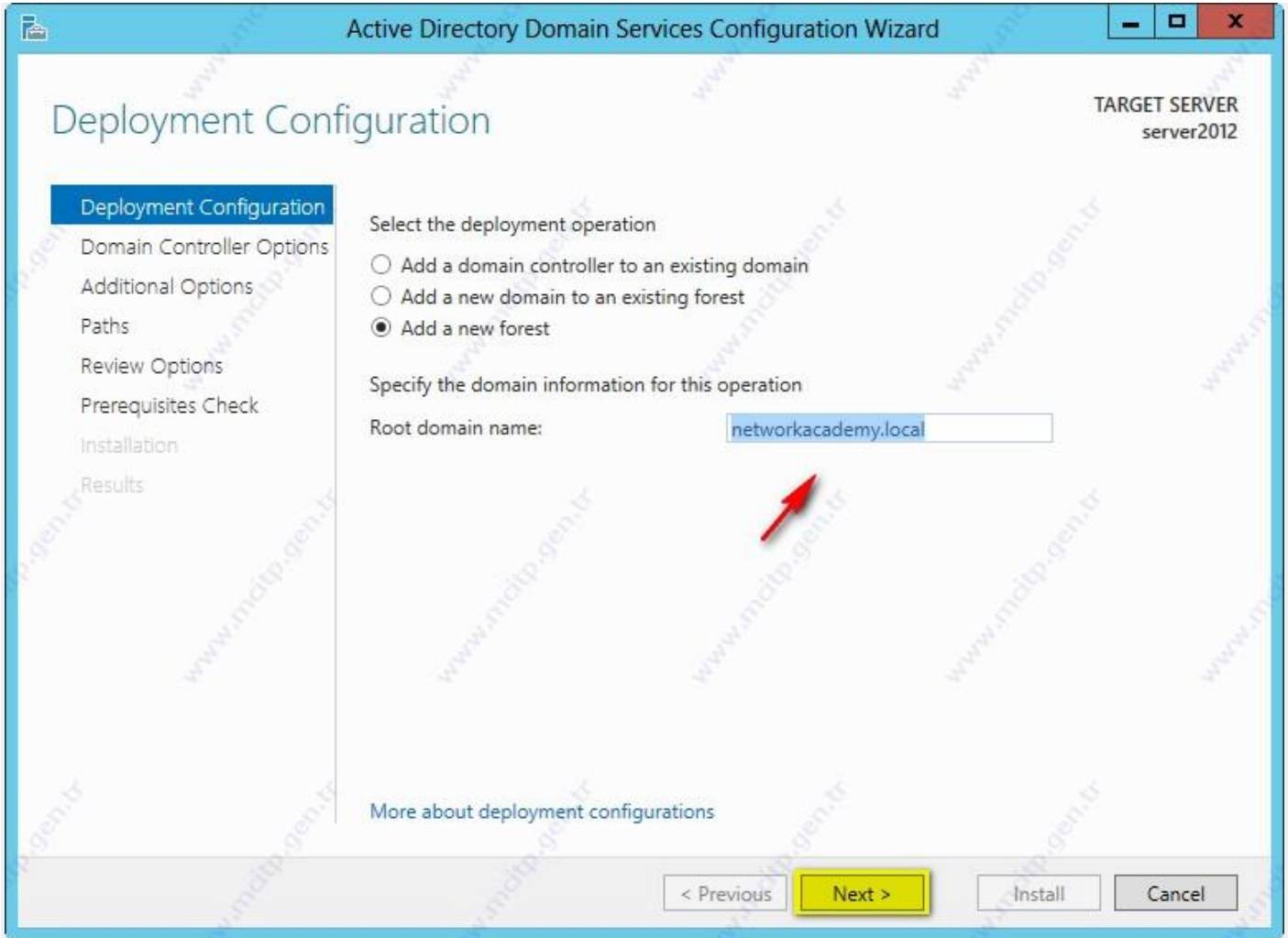
All Servers Task Details and Notifications

All Tasks | 1 total

Status	Task Name	Stage	Message	Action	Notifications
⚠	Post-deployment Configuration	Not Sta...	Configuration required for Active Directory Do...	Promote this server to a domain...	1

Status	Notification	Time Stamp
ℹ	Additional steps are required to make this machine a domain controller.	8/22/2012 11:01:14 PM

Promote this server to a domain controller : bu serveri DC 'ye yükselt.



Buraya tıklatınca AD konfigurasyonwizardı başlıyor.

Evet gördüğünüz gibi server 2012 ile activedirectory kurulum arayüzü biraz değişti.

Configurationwizardda ilk olarak

Add A newForest diyoruz ve domainimizin adını yazıyoruz.Burada domain ismi verirken kesinlikle DNS standartlarına uygun bir isim vermek zorundayız.Bunlardan en önemlisi domain ismi verirken uzantı olarak **.local**, **.com**, **.net**, **.com.tr** gibi uzantıları kullanmak zorundayız fakat genelde iç networklerde .local uzantısı kullanılır ki bizde buna uygun olarak domainimize **networkacademy.local** adını vereceğiz.

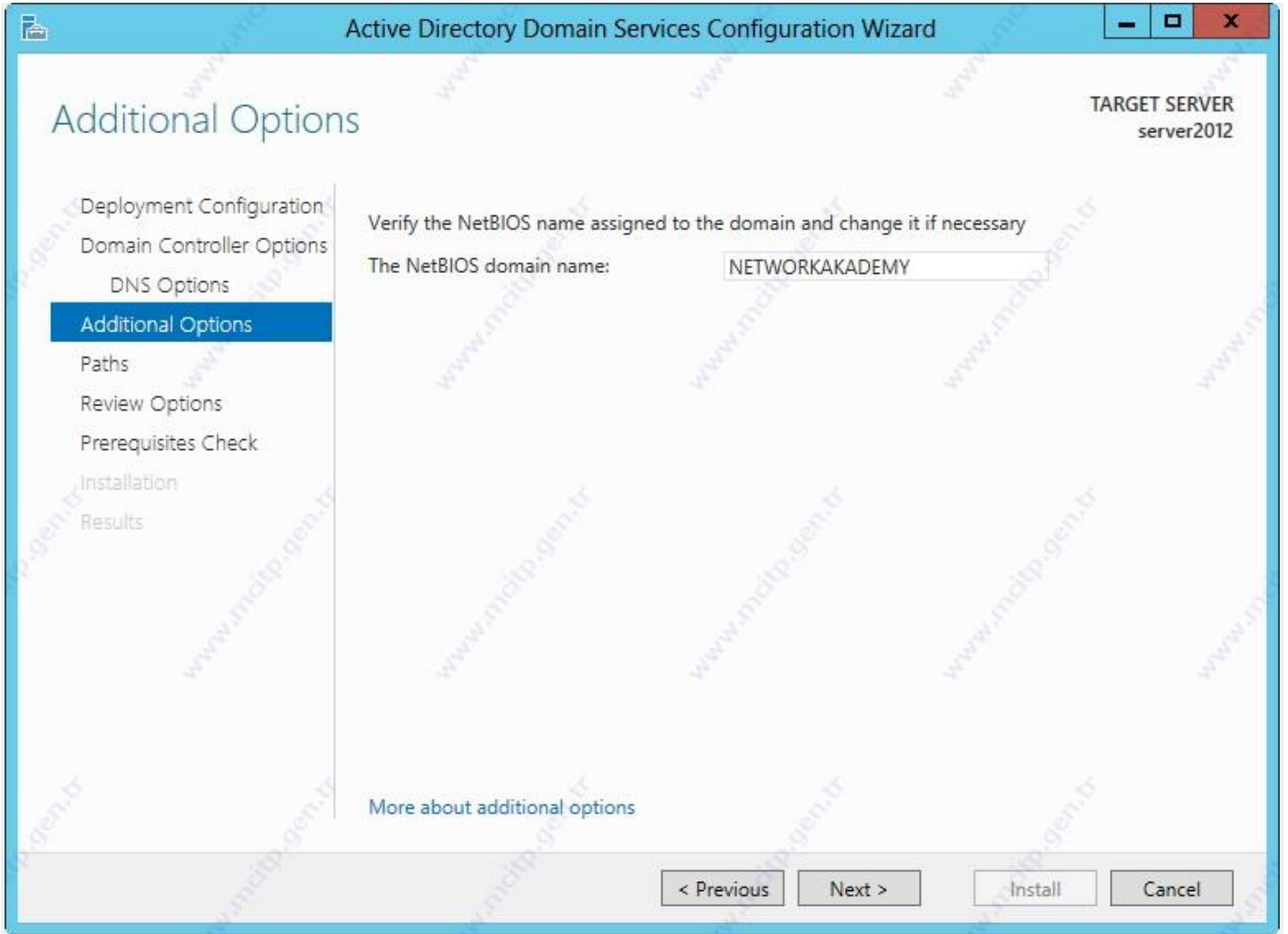
NEXT diyoruz

Burada **forestfunctionallevel** ve **domain functionallevel** 'ları seçiyoruz. Eğer ortamda farklı versiyonlarda DC yoksa (mesela 2000 DC, 2003 DC) server 2008 R2 seçilebilir. veya Daha üst seviye olan **server 12** seçilebilir.

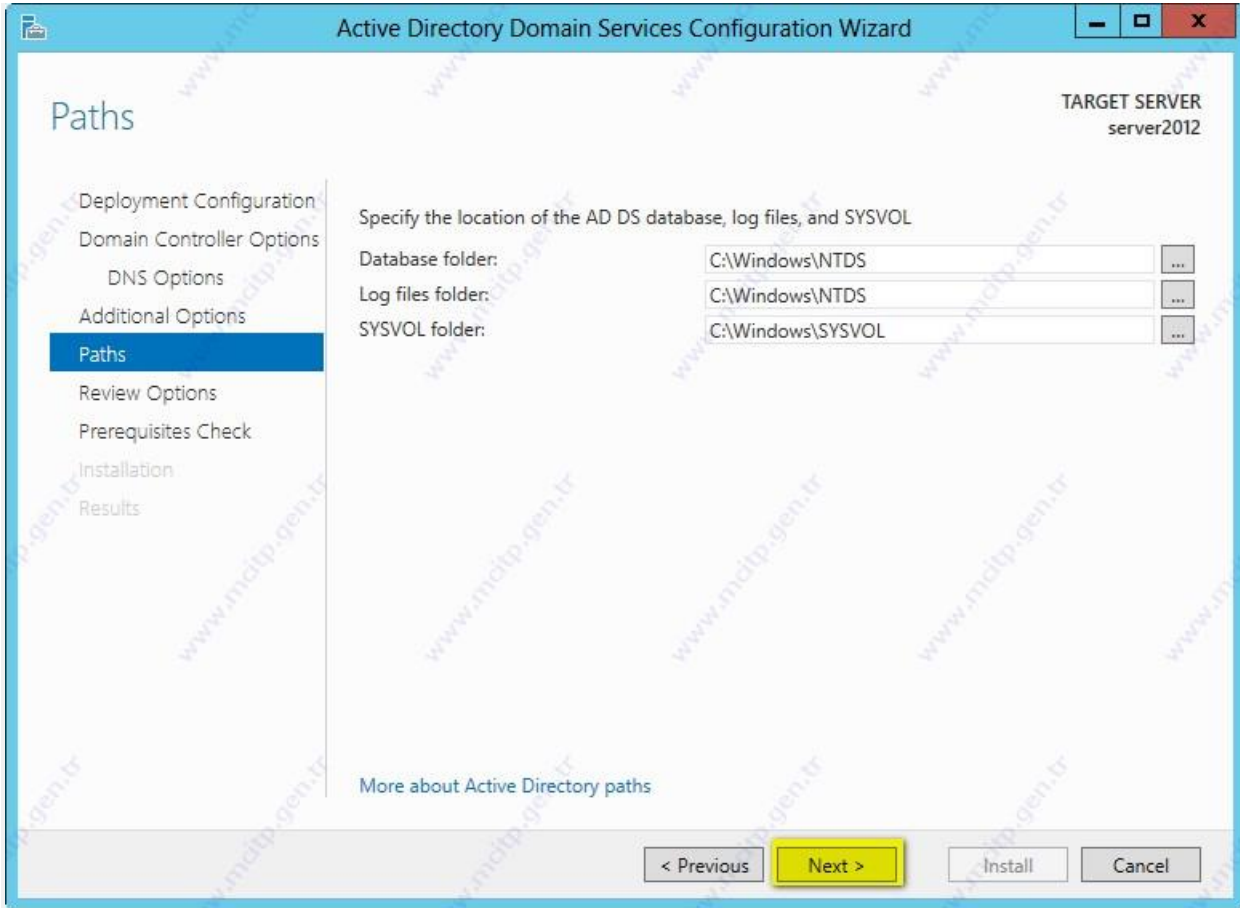
DNS kurulmasını istediğimizden **DNS** checkkoyuyoruz. **GlobalCatalog** zaten kurulması gereken bir servis olduğundan o default olarak işaretli geldi.

Burada **Directory Restore Modepasswordu** soruluyor. Bu password DC çöktüğünde ve Active Directory çalışmadığında kullanılacak localAdmin şifresidir .Bu arada vermekte ve unutmamakta fayda var. Başka bir makalemizde Active Restore Mode anlatacağım. Next diyoruz.

DNS Delegation kısmı ,burada çok büyük DNS zonaları olsaydı onları bolmek için kullanabilirdik fakat suan için **parentzone** (ana bolge) biz olacağımızdan **next** deyip geçiyoruz.



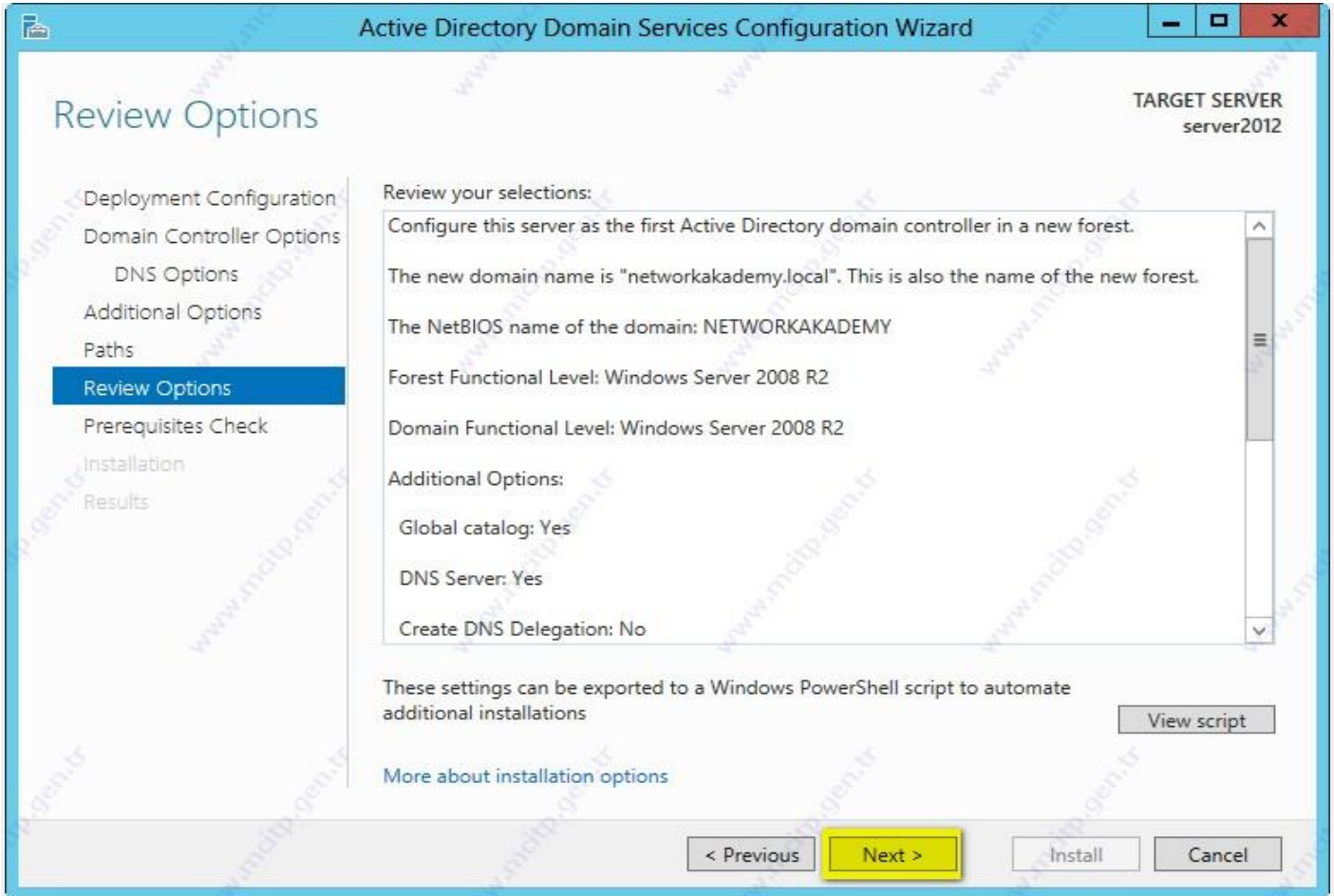
Burada domainimizin **NetBIOS** ismine karar veriyoruz. NetBIOS name tek olmak zorunda .**Next** diyoruz.



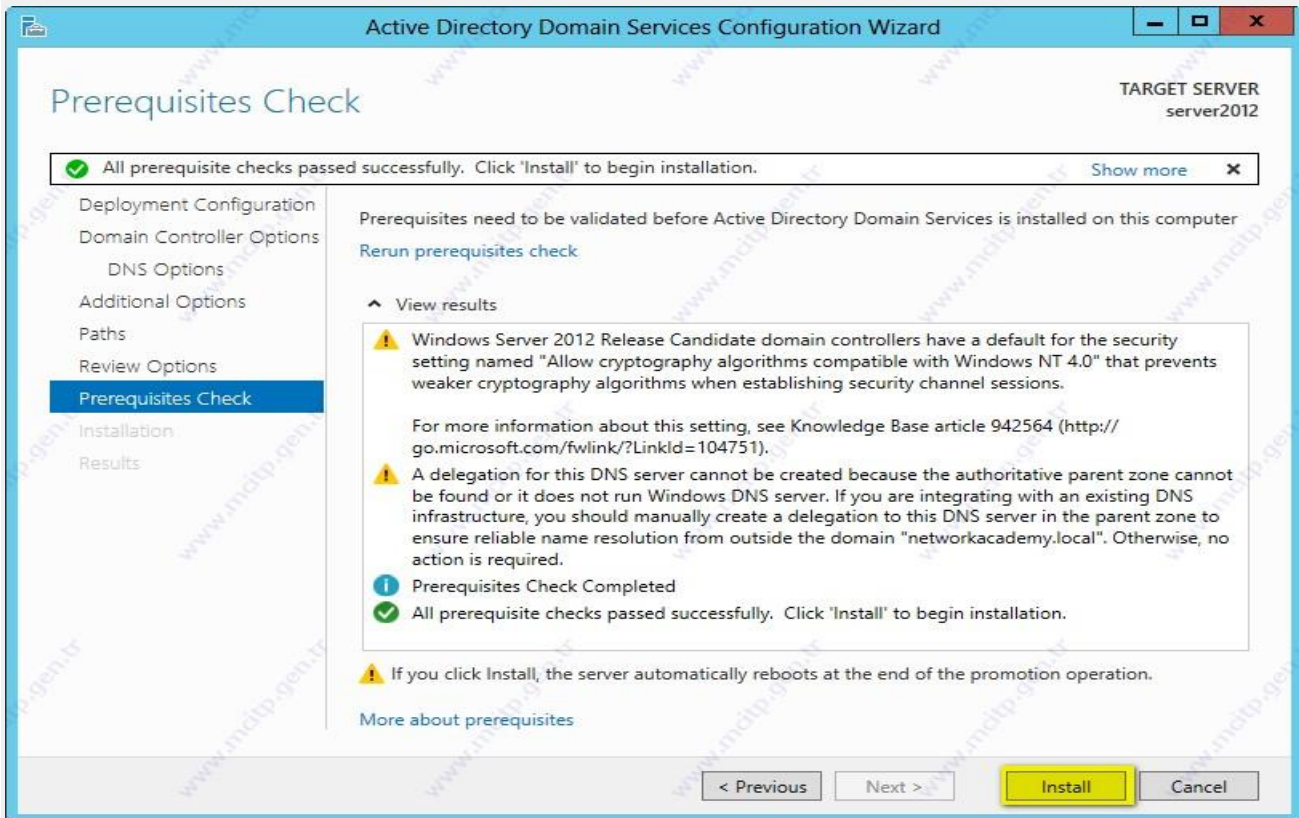
Burada Active Directory'nin kurulacağı klasörleri belirliyoruz.

Active Directory Database ve logların kurulacağı klasör ile Sysvol'un kurulacağı klasörler default olarak C: de kurulur fakat buradan değiştirilebilir.

Burada **Sysvol** klasörü çok önemlidir. Çünkü içerisinde group policy ayarları vardır. **Next** diyoruz.



Burada Next deyip kurulumu başlatabilir .Biz **next** diyoruz.



Öncelikle gereksinimleri (prerequisites) kontrol ederek ,bunların sağlanıp sağlanmadığını kontrol ediyor wizard ve gerekli uyarı yaptıktan sonra ,eğer gereksinimler yeterliyse ve sağlanıyorsa **install** diyerek Active Directory kurulumu başlatıyoruz.

Kurulum başarılı bir şekilde bittikten sonra serverirestart ediyoruz.



Window Server 2012 makinemiz restart olduktan sonra domain ismimizle login oluyoruz.